

UPCS®

The Unclaimed Property Compliance System



# Security Administrator Reference Guide Version 6.1.5



*UPCS® is a registered trademark of  
Chesapeake System Solutions, Inc.  
Proprietary and Confidential*



## Trademarks

T-Recs®, SmartAnalysis®, SmartMatch®, SmartResolve®, UPCS®, SmartTreasury® and Chesapeake System Solutions, Inc.® are registered trademarks of Chesapeake System Solutions, Inc.®. Chesapeake IDM™, SmartAudit™, NetResolve™ are trademarks of Chesapeake System Solutions, Inc.

Windows®, Windows 98/ME/NT/2000/XP® are registered trademarks of Microsoft, Inc. Other trademarks referenced are the property of their respective owners. All trademarks are used for identification purposes and do not establish an affiliation or sponsorship by the trademark owners of Chesapeake's products and services.

## Copyright

All Software, Documentation, and other Materials provided by Chesapeake are Copyright © 1995 - 2012, Chesapeake System Solutions, Inc.®. unless otherwise stated. All copyrights of third parties used with permission or under license.

## Address

Two Owings Mills Corporate Center  
10461 Mill Run Circle  
Suite 600  
Owings Mills, Maryland 21117

## Main Office

410-356-6805

## Product Support

410-356-6805

## After Hours Product Support

1-800-395-4528

## Fax

410-356-7625

All rights reserved.

Printed in the United States of America.

## Notice

The manual and any accompanying material (Documentation) are being made available to the Client in conjunction with the Client's use of the System described herein, in accordance with the

Client's agreement with Chesapeake System Solutions, Inc. (Chesapeake). This documentation is made conditionally available to the extent that receipt and acceptance limits its use to the purpose stated above and that the information contained herein is maintained on a confidential basis without disclosures to third parties. All parties accepting this material thereby agree not to reproduce, copy, or otherwise distribute this information without the express written consent of Chesapeake.

## Disclaimer

The information provided in this Document and by our customer support personnel is not intended as legal or accounting advice. If such advice is required, the services of a competent professional should be sought.

## Publication Data

Last Revised: March 2013

Publication Title: UPCS® 6.1.5 Security Administrator Reference Guide

# Security Administrator

## Version 6.1.5 Reference Guide

|   |    |
|---|----|
| Getting Started.....  | 1  |
| About the Security Administrator.....   | 1  |
| <i>Security Administrator Quick Look Guide</i> .....  | 2  |
| Getting Started with the Security Administrator .....   | 2  |
| <i>Security Administrator Toolbar</i> .....   | 4  |
| Defining and Maintaining Groups and User Accounts .....   | 5  |
| <i>Adding a Group</i> .....   | 5  |
| <i>Adding a User</i> .....  | 6  |
| <i>Viewing User Properties</i> .....  | 8  |
| <i>Viewing Active Users</i> .....   | 10 |
| <i>Assigning a User to a Different Group</i> .....  | 12 |
| <i>Locking Users</i> .....  | 13 |
| <i>Unlocking Users</i> .....  | 14 |
| <i>Deleting a Group</i> .....   | 15 |
| <i>Deleting a User</i> .....  | 17 |
| Passwords .....   | 18 |
| <i>Resetting Passwords</i> .....  | 18 |
| <i>Changing Passwords</i> .....   | 19 |
| Global Settings.....  | 19 |
| <i>Restricting UPCS Sessions</i> .....  | 20 |
| <i>Setting Password Requirements</i> .....  | 21 |
| <i>Enabling Single Sign On</i> .....  | 22 |
| Applying Group Security .....   | 24 |
| <i>Data and Access Security Restrictions</i> .....  | 24 |
| Use of any data-level restrictions.....   | 24 |
| Data-level restrictions based on Holder only, with no other data-level restrictions .....                         | 24 |
| Data-level restrictions in addition to or instead of Holder will not have access to the following functions ..... | 24 |
| Data-level restrictions not including Holder.....   | 25 |
| Inquire Only Access .....   | 25 |
| <i>Applying Data Security</i> .....   | 25 |
| <i>Applying Functional Security</i> .....   | 27 |

|   |    |
|---|----|
| <i>Changing the Status of Secured Items</i> .....       | 28 |
| <i>Applying Access and Dollar Amount Security</i> ..... | 29 |
| Applied Restrictions Overview .....                     | 31 |
| <i>User Locked</i> .....                                | 31 |
| <i>Session Locked</i> .....                             | 31 |
| <i>Data Security Results</i> .....                      | 33 |
| <i>Functional Security Results</i> .....                | 34 |
| <i>Inquiry Only Access Type</i> .....                   | 35 |
| Customer Support Phone Numbers .....                    | 36 |
| Index .....   | 37 |

## **Getting Started**

The UPCS Security Administrator Reference Guide provides information on the UPCS Version 6.1.5 Security features. These features provide more precise levels of security so you can now restrict access based on the criteria of your choosing. This document summarizes the features and functionality of the Security Administrator, providing step-by-step instructions to guide you through the processes.

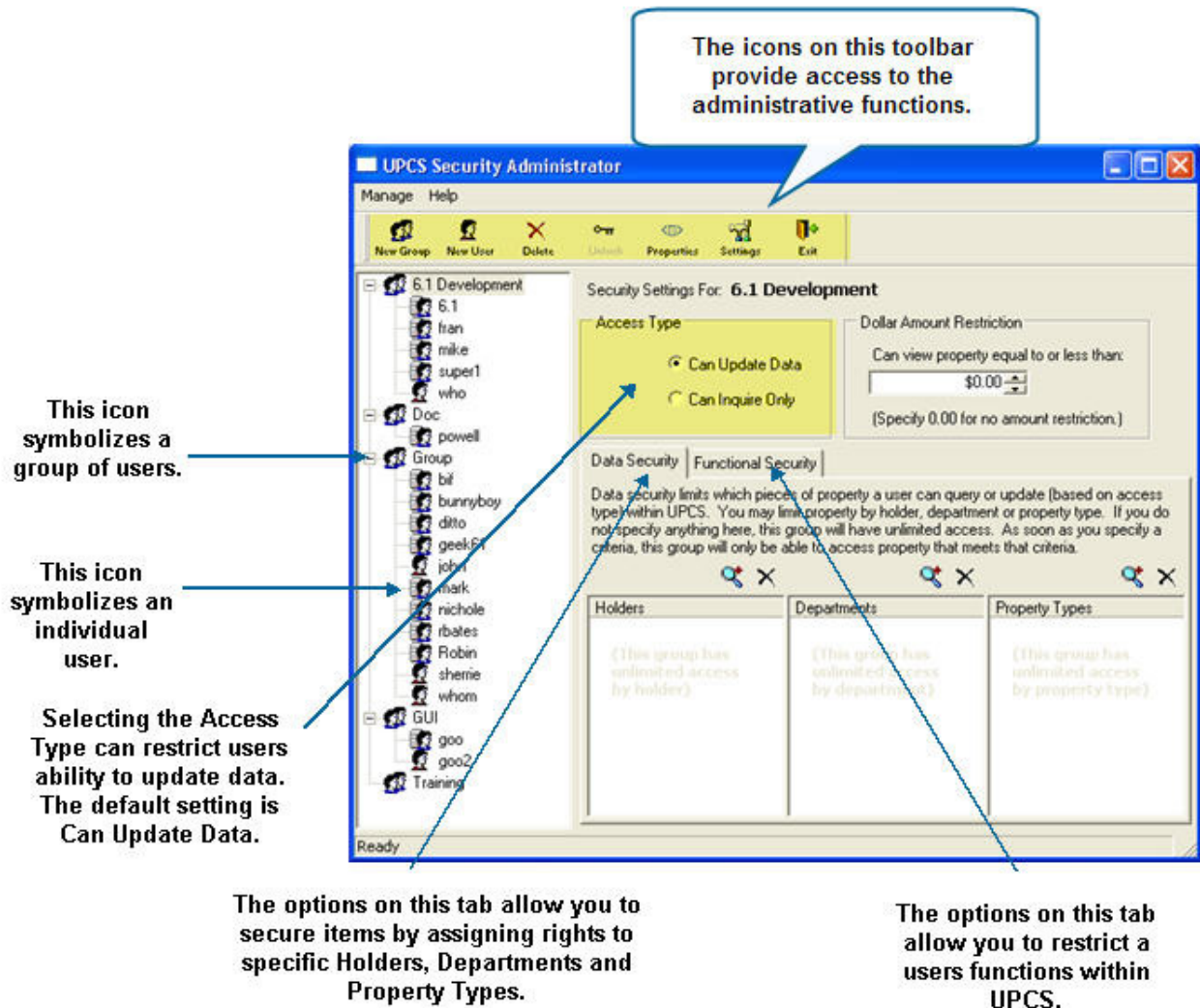
## **About the Security Administrator**

User accounts are managed using the Security Administrator, which is only installed when an administrator type installation of UPCS is selected. Any user with this type of installation is considered a UPCS Administrator and has rights to define UPCS groups and user accounts. These groups and accounts can be maintained at any time, as changes to your business practices require.

Security is administered on user groups. This means a group must be created prior to the creation of a user account and all members within a group have the same profile. If a user requires a different profile than the rest of the group, this user constitutes a different group. Each user has a unique username and password. Users have access to all functions within UPCS when originally created. Maintaining these accounts is an Administrator function and only those individuals whose security profiles allow access are able to update these groups and users. Changes made in the Security Administrator are effective immediately.

The two primary ways to make security assignments are Data Security and Functional Security. Data Security is used to assign access based on specific data-level criteria. Access is unlimited until criteria are specified. You may assign rights by holder, department, or property type. Functional Security is used to set limitations on entire areas or functions in UPCS by disabling them or making them invisible to the selected group. You may additionally restrict users by applying Inquire Only access and/or a Dollar Amount Restriction.

## Security Administrator Quick Look Guide

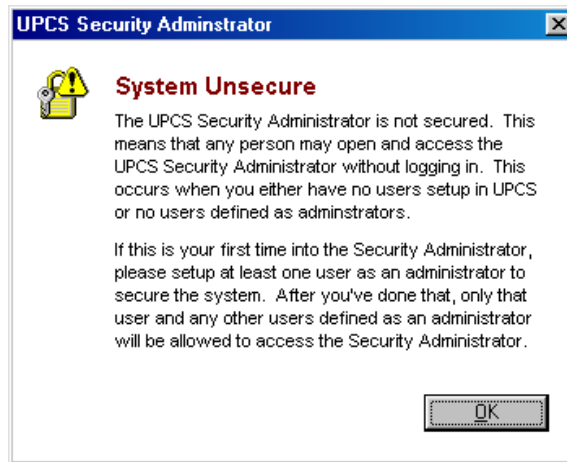


## Getting Started with the Security Administrator

Once you have successfully installed UPCS 6.1.5, a shortcut will be placed in the Start Menu to access the Security Administrator.

1. Select **Programs > Chesapeake's Unclaimed Property Suite > Security Administrator**.

The first time you access the Security Administrator, you will receive notification that the system is not secure.



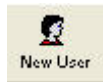
This means that anyone with access to the Security Administrator may open the UPCS Security Administrator without logging in. This occurs when you either do not have users setup in UPCS or no users defined as administrators. To secure the system, you must designate at least one user as an administrator. This will allow only the user(s) with administrative rights to access the Security Administrator. If you choose not to assign administrators, you will still be able to access the Security Administrator; however, you will continue to receive the System Unsecure message until an administrator is designated.

## Security Administrator Toolbar

This toolbar is always available at the top of the Security Administrator window. Each icon offers access to the desired Administrative feature. These options are also available using the Navigation Toolbar Options.



*Navigation Toolbar*



Select this icon to create a new user account within a group.



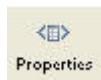
Select this icon to create a new user group.



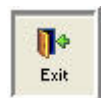
Select this icon to unlock a locked user account



Select this icon to define general session restrictions, define user locking requirements and establish password requirements. Settings made here will apply to all users.



Select this icon to reset user passwords and view general user account information including name, description, email address, password and date/time of last login.



Select this icon to exit and close the UPCS Security Administrator application.

## Defining and Maintaining Groups and User Accounts


Groups and user accounts are set up using the Security Administrator. These groups and accounts can be maintained at any time, as changes to your business practices require.

Security is administered on user groups. This means a group must be created prior to the creation of a user account and all members within a group have the same profile. If a user requires a different profile than the rest of the group, this user constitutes a different group. Each user has a unique username and password. Users have access to all functions within UPCS when originally created. Maintaining these accounts is an Administrator function and only those individuals whose security profiles allow access are able to update these groups and users. Changes made in the Security Administrator are effective immediately.

### Adding a Group

A group must be created prior to the creation of the user accounts since users are set up within a group. User accounts are organized alphabetically within their group. Criteria apply to an entire group, so it is important to make sure users are assigned to a group matching their security rights.

To add a new group:

1. Select  on the toolbar or select **Manage > New > Group**. The New Group dialog box displays.



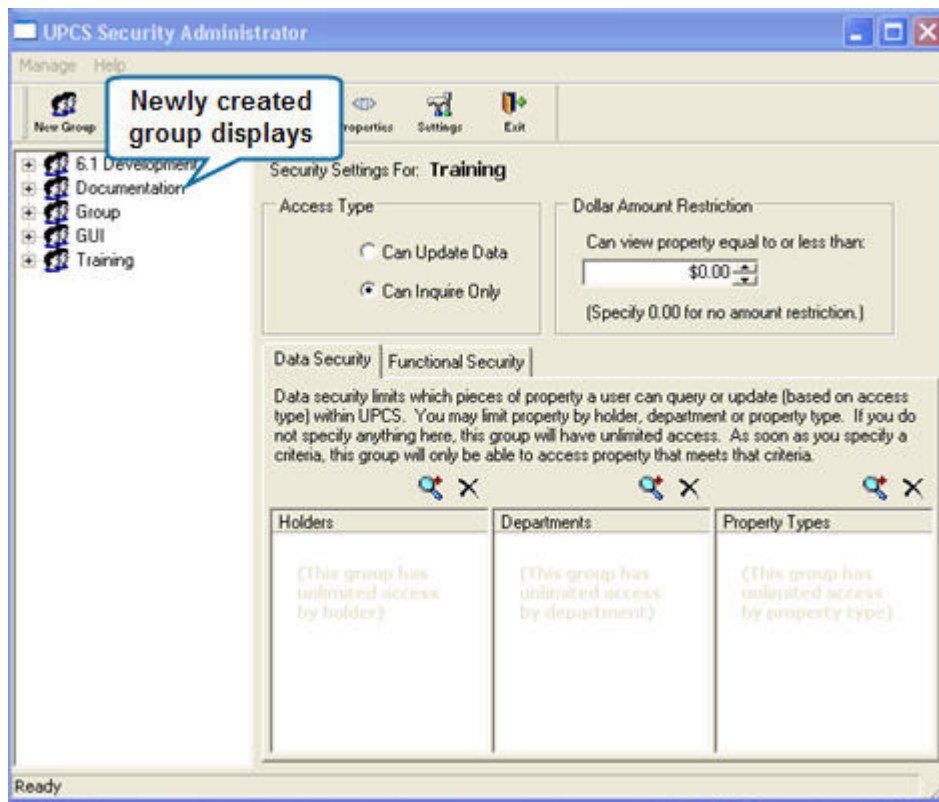
*New group Dialog*

2. Enter a **name** for the group.
3. Select **OK**. The New Group Created message displays with the new group name.



*New Group Created Message*

4. Select **OK**. UPCS displays the new group in the left hand column.



*Newly Created Group Displays*

## Adding a User

User accounts are created within a group. Duplicate user IDs are not allowed. Each user must have a unique ID. See the *Changing Passwords* section in this chapter for instructions on changing passwords.

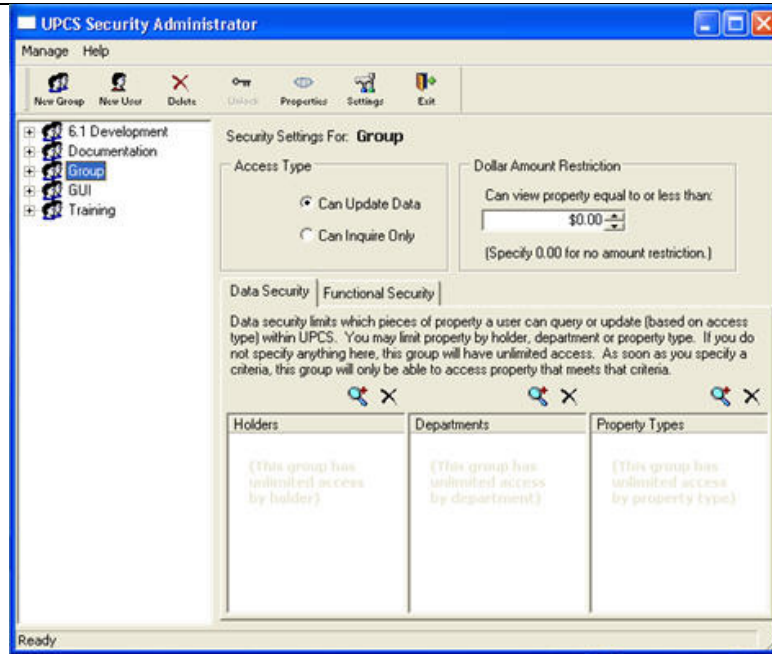
---

**NOTE:** Users are required to change their password at first login.


---

To add a new user:

1. Highlight the group name to which you want to add a user.



Highlight Group Name

2. Click  on the toolbar or select **Manage > New > User**. UPCS displays a New User dialog box.
3. Enter a **name** for the user in the dialog box.

Create User Dialog

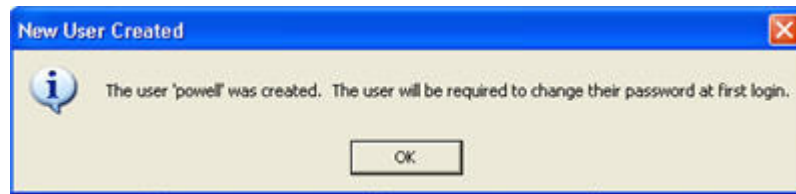
4. Enter an **Initial Password** for the user and confirm initial password. The user will be forced to change the password at first login.
5. Enter the password again to **Confirm Initial Password**.
6. Enter an **Email Address** for the user.

**NOTE:** UPCS 6.1.5 uses email addresses from the Security Administrator to send notifications from the Compliance Calendar. If you do not enter an email address, the user will not be able to receive these notifications. See Using the Compliance Calendar in the User Manual for more information on the Compliance Calendar.

7. Select **Administrator** to assign privileges to the Security Administrator.

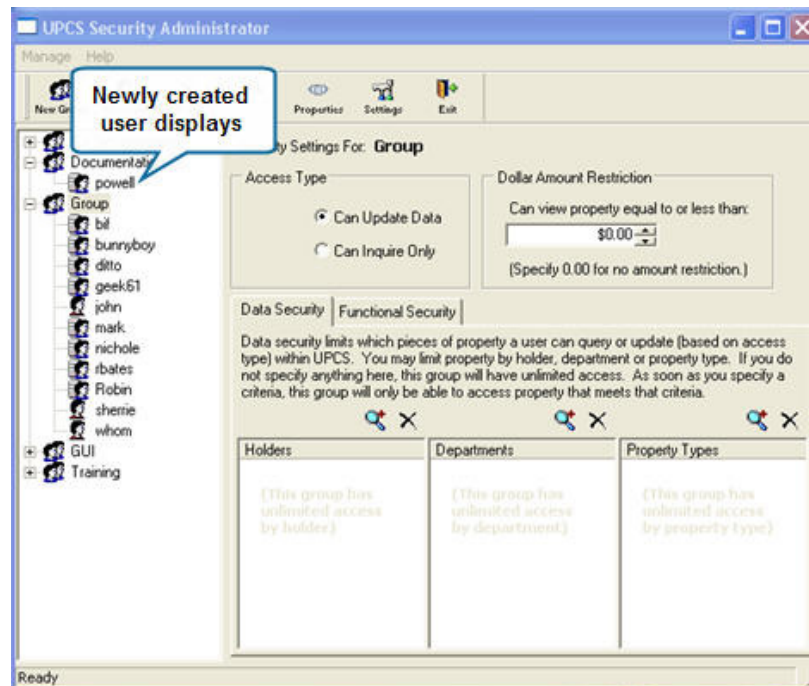
**NOTE:** The user must be designated as Administrator during installation. If no Administrator is designated, all users with the Security Administrator installed will have access and the Security Administrator will remain unsecured. Otherwise, only designated administrators will have access.

7. Select **OK**. The New User Created message displays.



*New User Created Dialog*

8. Select **OK**. UPCS displays the new user in the left hand column.



*New User Displays*

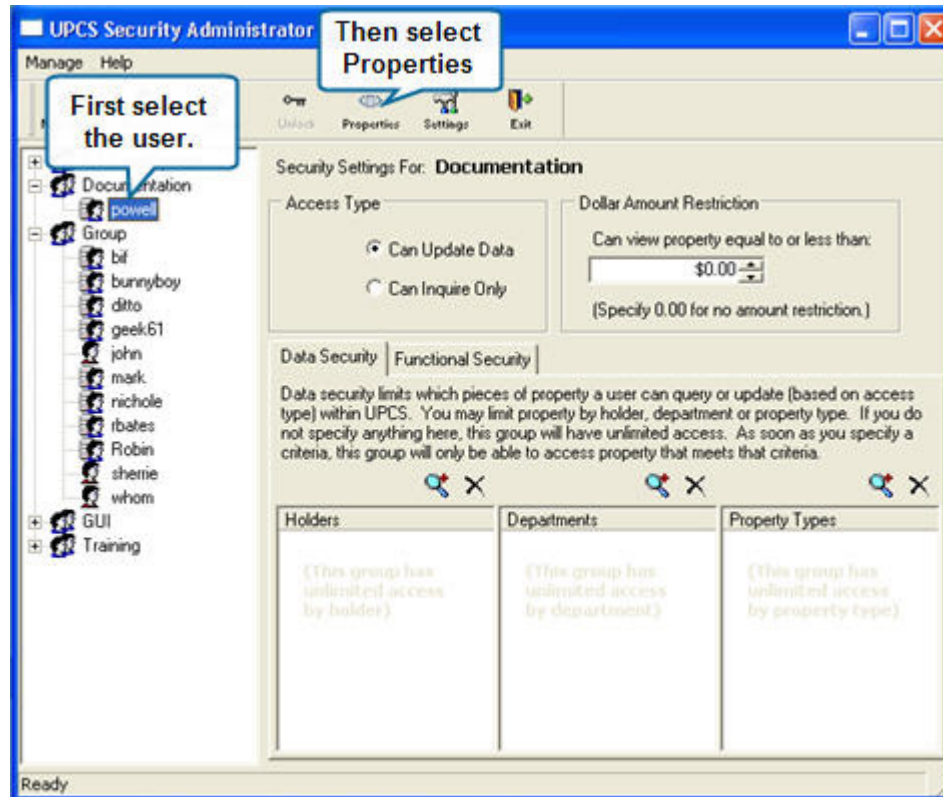
## Viewing User Properties

User account properties include name, email address, and password. You may use this feature to view and edit these properties with the exception of the user password, which


can only be changed by the user within UPCS. You may, however, reset this password to 'UPCS' if necessary.

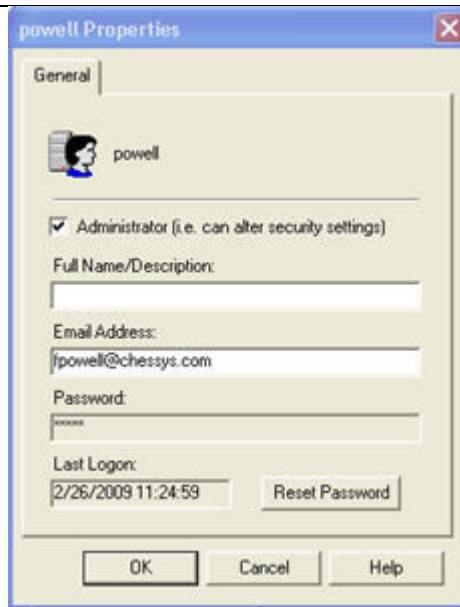
To view user properties:

1. Select the **user** whose account properties you wish to view.



*Select the User then Properties*

2. Select  **Properties** on the UPCS toolbar or select **Manage > Properties**. The properties for the selected user displays.



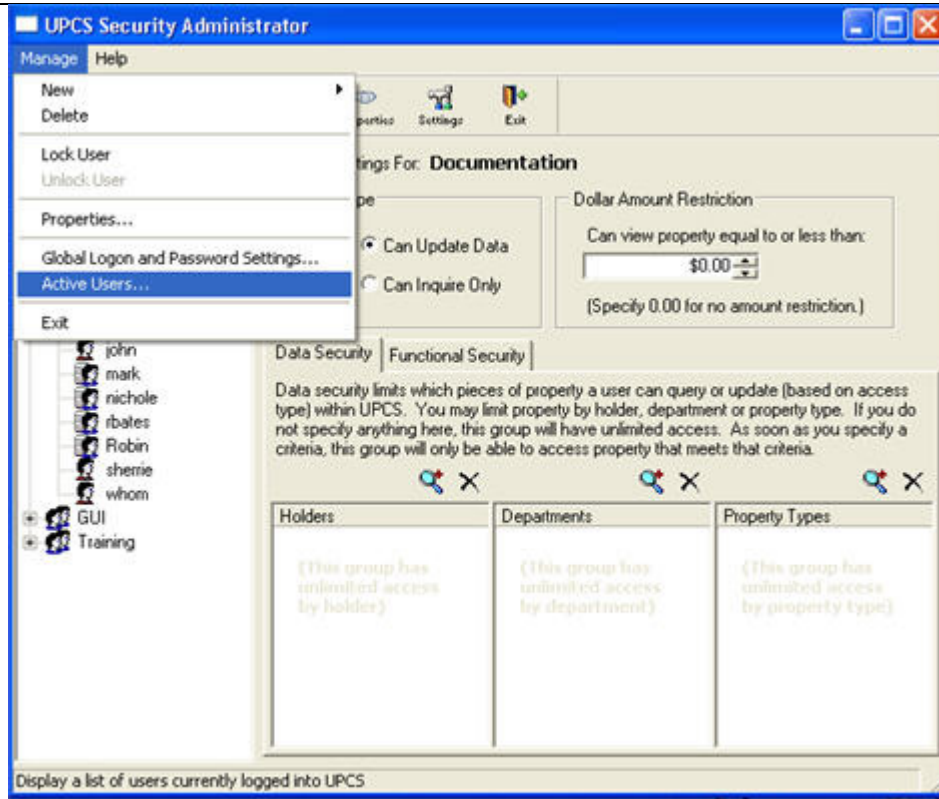
*User Properties*

3. Edit the fields that require revision.
4. Select **OK** to save the changes. UPCS returns to the Security Administrator.

## Viewing Active Users

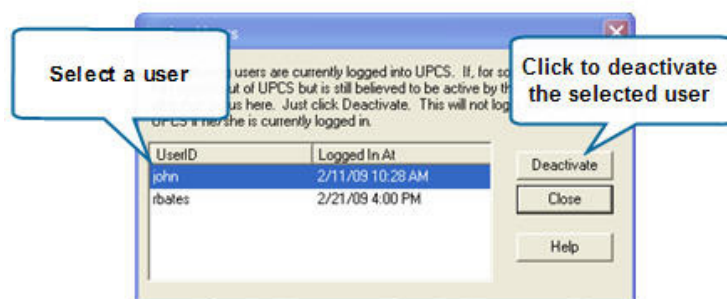
The Security Administrator allows you to view a list of users currently logged into UPCS. This list provides the User IDs as well as the login time and date. You may use this function to deactivate a user who has logged out of UPCS but is still believed to be active by the system. Deactivating a user does not terminate valid sessions.

To view the list of active users:



Manage &gt; Active Users

1. Select **Manage > Active User**. The Active Users list displays the users that are currently logged into UPCS. If for some reason, a user has logged out of UPCS but is still believed to be active by the system you may alter that status here by deactivating the user. This will not log a user out of UPCS if they are currently logged in. Continue with steps 2-3 if you want to deactivate a user listed.
2. Select the user you want to deactivate.



Deactivate User

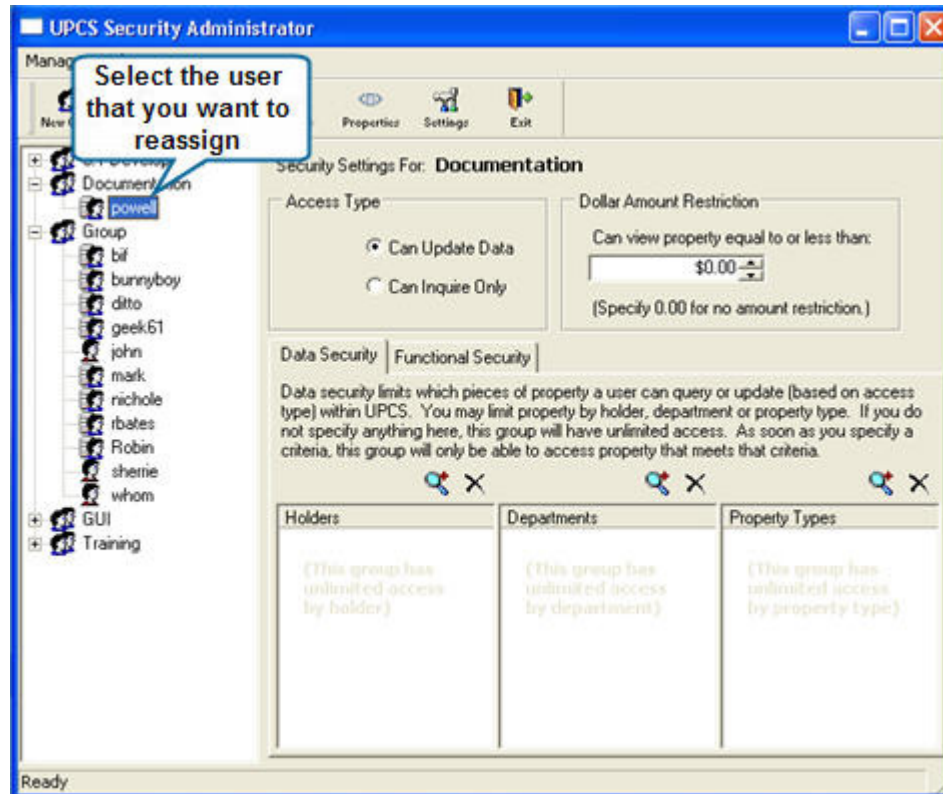
3. Select **Deactivate**. UPCS deactivates the selected user.

## Assigning a User to a Different Group

Users can be reassigned to a different group at any time. This is helpful if an individual's rights change to match a different group or if you want to delete a group, but do not want to delete all users. This option allows you to move the user to another existing group.

To assign users to a different group:

1. Select the user that you want to move.



ERROR: stackunderflow  
OFFENDING COMMAND: ~

STACK: